UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/686,331	10/14/2003	Richard M. Butler	10991268-3	7201

22879 7590 09/23/2005

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
DO, CHAT C	

ART UNIT	PAPER NUMBER
2193	

DATE MAILED: 09/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/686,331	BUTLER, RICHARD M.	
	Examiner	Art Unit	
	Chat C. Do	2193	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *07/28/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This communication is responsive to Amendment filed 07/28/2005.

2. Claims 1-22 are pending in this application. Claims 1 and 22 are independent claims. This Office Action is made final after a RCE filed 07/28/2005.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-2 and 7-21 are rejected under 35 U.S.C. 103(a) as being obvious over Edelkind et al. (U.S. 5,987,483) in view of Nozuyama (U.S. 5,867,409).

Re claim 1, Edelkind et al. disclose in Figure 4 a method of generating a random number, comprising: a) retrieving values from a number of random generators (200) which are coupled to a number of microprocessor buses and a step of generating a random number which is based on the values retrieved from the number of random generators (300). Edelkind et al. do not disclose the random number generator is a MISR. However, Nozuyama discloses in Figure 2 random number generator is a MISR. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to replace a multiple random number generators with a

multiple MISRs as disclosed in Nozuyama's Figure 2 into Edelkind et al.'s Figure 4 because it would enable to increase the randomness and performance of the system random output.

Re claim 2, Edelking et al. further disclose the number of MISRs is one (200 in Figure 4).

Re claim 7, Edelking et al. further disclose one of the number of MISRs is coupled to a bus which runs wholly within an integrated circuit package (200 and 300 in Figure 4).

Re claim 8, Edelking et al. further disclose retrieving values from the number of MISRs comprises: a)loading bits of a value stored in a first of the number of MISRs, in parallel, into a temporary register (input into 300); and b)retrieving the value stored in the temporary register (output of 300 and col. 5 lines 45-50).

Re claim 9, Edelking et al. further do not disclose retrieving values from the number of MISRs comprises retrieving a value from a first of the number of MISRs by stepping the first of the number of MISRs to serially shift a plurality of bits out of the MISR. However, Nozuyama discloses in Figure 1 an output of MIRS is serially shifted out (output of XOR). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to replace a multiple random number generators with a multiple LFSRs as disclosed in Nozuyama's Figure 1 into Edelkind et al.'s Figure 4 because it would enable to increase the randomness of the system random output.

Re claim 10, Edelking et al. further disclose generating a random number comprises hashing together the values retrieved from the number of MISRs (300).

Re claim 11, Edelking et al. do not disclose generating a random number comprises XORing the values retrieved from the number of MISRs. However, Nozuyama discloses in Figures 1-2 that all the output data are exclusiveORed together to form a new output random data. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to add a XOR for XORing all the values retrieved as disclosed in Nozuyama's Figures 1-2 into Edelkind et al.'s Figure 4 because it would enable to increase the randomness of the system random output.

Re claim 12, Edelking et al. do not disclose a initializing each of the number of MISRs upon boot of a computer in which the MISRs reside. However, the examiner takes an official notice that these flip-flops only hold the data when the power is on so the flip-flops will reset upon power initialization. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to initialize the MISR upon the power reset because it would enable to start a new sequence of random number.

Re claim 13, Edelking et al. further disclose values are retrieved from the number of MISRs via an operating system call (310 and col. 5 lines 47-50).

Re claim 14, Edelking et al. further disclose operating system call is of a highest privilege level (col. 5 lines 49-52).

Re claim 15, Edelking et al. further disclose generating a random number is performed substantially immediately after the number of MISR readings are taken, the method further comprising storing (300) the random number in a temporary location for subsequent use (output of 300).

Re claim 16 and 18, Edelking et al. do not disclose operating system call is issued in response to an application's request for a random number. However, the examiner takes an official notice that it is obvious operating system call is issued in response to an application's request for a random number as a request for encrypting a key for security reason upon the user request. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to generate a random number upon user's request because it would enable to save the computation and increase the reliability of the random numbers.

Re claim 17, Edelking et al. do not disclose the retrieved values from a number of MISRs comprises a computer program's issuance of a request to read the number of MISRs. However, Nozugama discloses that the retrieved values from a number of MISRs comprises a computer program's issuance of a request to read the number of MISRs (col. 1 lines 35-40). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to add a program's issuance as disclosed in Nozugama into Edelking et al.'s invention because it would enable to test the output of the random system prior outputting.

Re claims 19-21, Edelking et al. do not disclose the test program. However, Nozugama discloses a testing the MISR (BIST) by: a) initializing the number of MISRs

to known values (reason as in claim 12); b) executing a test program on the microprocessor in which the number of MISRs reside (col. 1 lines 35-45) c) retrieving values from the number of MISRs; d) comparing the values retrieved from the number of MISRs with expected values; and e) indicating a failure of one of the number of MISRs if its retrieved value does not agree with its expected value (col. 1 lines 49-52). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to add a test program (BIST) as disclosed in Nozugama into Edelking et al.'s invention because it would enable to test the output of the random system prior outputting.

5. Claims 3-6 are rejected under 35 U.S.C. 103(a) as being obvious over Edelkind et al. (U.S. 5,987,483) in view of Nozuyama (U.S. 5,867,409), as applied to claim 1 above, in further view of Thomlinson et al. (U.S. 5,778,069).

Re claims 3-6, Edelking et al. in view of Nozuyama disclose that the input data to the MISR is a input data (IN0-IN7 in Figure 2), but do not disclose one of the number of MISRs is coupled to a data bus / address bus / instruction data / instruction address which transfers data between a data / address / instruction data / instruction address cache and a CPU core. However, Thomlinson et al. disclose in Figure 3 (col. 3 lines 15-30) that the input data can be anything from the static bits (52), machine bits (54), and application bits (56). Therefore, it would have been obvious application to a person having ordinary skill in the art at the time the invention is made to input a data, address, instruction data, or instruction address as the input data to one of number MISRs as disclosed in

Thomlinson et al.'s invention into Edelking et al. in view of Nozuyama's invention because it would increase the randomness for generating a random number from multiple random sources (col. 3 lines 30-35).

6. Claim 22 is rejected under 35 U.S.C. 103(a) as being obvious over Nozuyama (U.S. 5,867,409) in view of Edelkind et al. (U.S. 5,987,483).

Re claim 22, Nozuyama discloses in Figures 3 and 7 a method of generating a random number comprising: assigning a built-in self-test (BIST) (col. 1 lines 35-40) local block of a microprocessor a major address (d_0-d_{n-1} in Figure 3), assigning each of a number of multiple input shift registers (MISRS) in the BIST local block a minor address (each individual data d_x), issuing an instruction to turn on and initialize the MISRS, issuing a request to read the MISRS, in response to a request for an XoRing the MISR readings with each other (Figure 3), and with historical readings, if any, to generate. Nozuyama does not disclose the random number is used to generate the encryption key. However, Edelkind et al. disclose in column 1 lines 10-20 that the stable random number sequences is used in encryption key. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to use the random number in encryption key as disclosed in Edelkind et al.'s invention into Nozuyama's invention because it would enable to prevent detectable key.

Response to Arguments

7. Applicant's arguments with respect to claims 1-22 have been considered but are moot in view of the new ground(s) of rejection filed 01/28/2005.

Conclusion

8. This is a continuation of applicant's earlier Application No. 10/686,331. All claims are drawn to the same invention claimed in the earlier application and could have been finally rejected on the grounds and art of record in the next Office action if they had been entered in the earlier application. Accordingly, **THIS ACTION IS MADE FINAL** even though it is a first action in this case. See MPEP § 706.07(b). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no, however, event will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chat C. Do whose telephone number is (571) 272-3721. The examiner can normally be reached on M => F from 7:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chaki Kakali can be reached on (571) 272-3719. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Chat C. Do
Examiner
Art Unit 2193

September 14, 2005

KAKALI CHAKI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100